SPYWOLF

Security Audit Report

Completed on

August 6, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **Rich Doge Poor Doge** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

"

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

– SPYWOLF Team –

TABLE OF CONTENTS

RICH DOGE

POOR DOGE

PROJECT DESCRIPTION

According to their roadmap:

Rich Doge Poor Doge is a project that will implement staking, RPDOGE merch, NFT and possible combat P2E game.

Release Date: Presale starts on August, 2022

Category: Staking

CONTRACT INFO

Token Name
Rich Doge Poor Doge

Symbol
R1CH

Contract Address
0x9758d54cB48D11dc5BBFD65dEb5a4Eb7B35aaB86

Network
Binance Smart Chain

Language
Solidity

Deployment Date
August 05, 2022

Verified?
Yes

Total Supply
241,000,000

Status
Not launched

TAXES

Buy Tax
12%

Sell Tax
12%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

02

CURRENT STATS

(As of August 05, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:
Not Launched!

MaxSellTxAmount
2,410,000

DEX:
PancakeSwap

LP Address(es)

Liquidity not added yet

03

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	241000000 R1CH
Median Transfer Amount	241000000 R1CH
Average Transfer Amount	241000000 R1CH
First transfer date	2022-08-05
Last transfer date	2022-08-05
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2022-08-05 19:32:44 UTC
Created	2022-08-05 19:32:44 UTC
Create TX	0x2f2614c2364c37223fbb180e20acfb3b5844 9b7bb13e41e32e6a0f6cd98721ac
Creator	0x5e3f9aef6bf1000b305e931ab70161167f18cf 61

FEATURED WALLETS

Owner address	0x5e3f9aef6bf1000b305e931ab70161167f18cf61
Dev wallet	0xd2b88ab1210157ace772f99d6dd4cdae5626b63f
Marketing wallet	0x50e1854a4002892eb4dc03dc0aaaefcd1a917f56
Ops wallet	0x8703fb7d8ada08d8927d3010da2c7137f6f67d1e
LP address	**Liquidity not added yet**

TOP 3 UNLOCKED WALLETS

1

100%   Same as owner

*Tokens are not distributed yet

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

07

FOUND THREATS

⚠️ Medium Risk

Owner can set buy/sell fees up to 20%.
Combined buy+sell=40%.

```
function SetBuyTaxes(
    uint256 _marketing,
    uint256 _liquidity,
    uint256 _ops,
    uint256 _dev
) external onlyOwner {
    taxes = Taxes(_marketing, _liquidity, _ops, _dev);
    require((_marketing + _liquidity + _ops + _dev) <= 20, "Must keep fees at 20% or less");
}

function SetSellTaxes(
    uint256 _marketing,
    uint256 _liquidity,
    uint256 _ops,
    uint256 _dev
) external onlyOwner {
    sellTaxes = Taxes(_marketing, _liquidity, _ops, _dev);
    require((_marketing + _liquidity + _ops + _dev) <= 20, "Must keep fees at 20% or less");
}
```

- Recommendation:
    - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

08-A

⚠️ Low Risk

Owner can set cooldown between sells up to 5 minutes.

```solidity
function updateCooldown(bool state, uint256 time) external onlyOwner {
    coolDownTime = time * 1 seconds;
    coolDownEnabled = state;
    require(time <= 300, "cooldown timer cannot exceed 5 minutes");
}

function _transfer(
address sender,
address recipient,
uint256 amount
) internal override {
..................
if (coolDownEnabled) {
    uint256 timePassed = block.timestamp - _lastSell[sender];
    require(timePassed >= coolDownTime, "Cooldown enabled");
    _lastSell[sender] = block.timestamp;
}
..................
}
```

08-B

ℹ️ Informational

Owner can exclude address from fees.

```solidity
function updateExemptFee(address _address, bool state) external onlyOwner {
    exemptFee[_address] = state;
}

function bulkExemptFee(address[] memory accounts, bool state) external onlyOwner {
    for (uint256 i = 0; i < accounts.length; i++) {
        exemptFee[accounts[i]] = state;
    }
}
```

Owner can change max transaction limit, but can't lower it than 0.1% of total supply.

```solidity
function updateMaxTxLimit(uint256 maxBuy, uint256 maxSell, uint256 maxWallet) external onlyOwner {
    require(maxBuy >= 241_000, "Cannot set max buy amount lower than 0.1%");
    require(maxSell >= 241_000, "Cannot set max sell amount lower than 0.1%");
    require(maxWallet >= 2_410_000, "Cannot set max wallet amount lower than 1%");
    maxBuyLimit = maxBuy * 10**decimals();
    maxSellLimit = maxSell * 10**decimals();
    maxWalletLimit = maxWallet * 10**decimals();
}
```

Owner can withdraw any tokens from the contract.

```solidity
function rescueBNB(uint256 weiAmount) external onlyOwner {
    payable(owner()).transfer(weiAmount);
}

function rescueBSC20(address tokenAdd, uint256 amount) external onlyOwner {
    require(tokenAdd != address(this), "Owner can't claim contract's balance of its own tokens");
    IBEP20(tokenAdd).transfer(owner(), amount);
}
```

08-C

GOOD PRACTICES

Rich Doge Poor Doge

GOOD PRACTICES FOUND

1. Consider fundamental tradeoffs

2. Be attentive to blockchain properties

3. Ensure careful rollouts

4. Keep contracts simple

5. Stay up to date and track development

✔ The owner cannot mint new tokens after deployment

✔ The owner cannot stop or pause the contract

✔ The owner can set a transaction limit, but can't lower it than 0.1% of total supply

09

According to Pinksale's presale page:

- 30% - Presale
- 20.5% - Liquidity
- 15% - CEX Reserves
- 10% - Staking
- 19.5% - Team
- 5% - Burnt

Tokens distribution

Staking
10,0%

Presale
30,0%

Liquidity
20,5%

CEX Reserves
15,0%

Burnt
5,0%
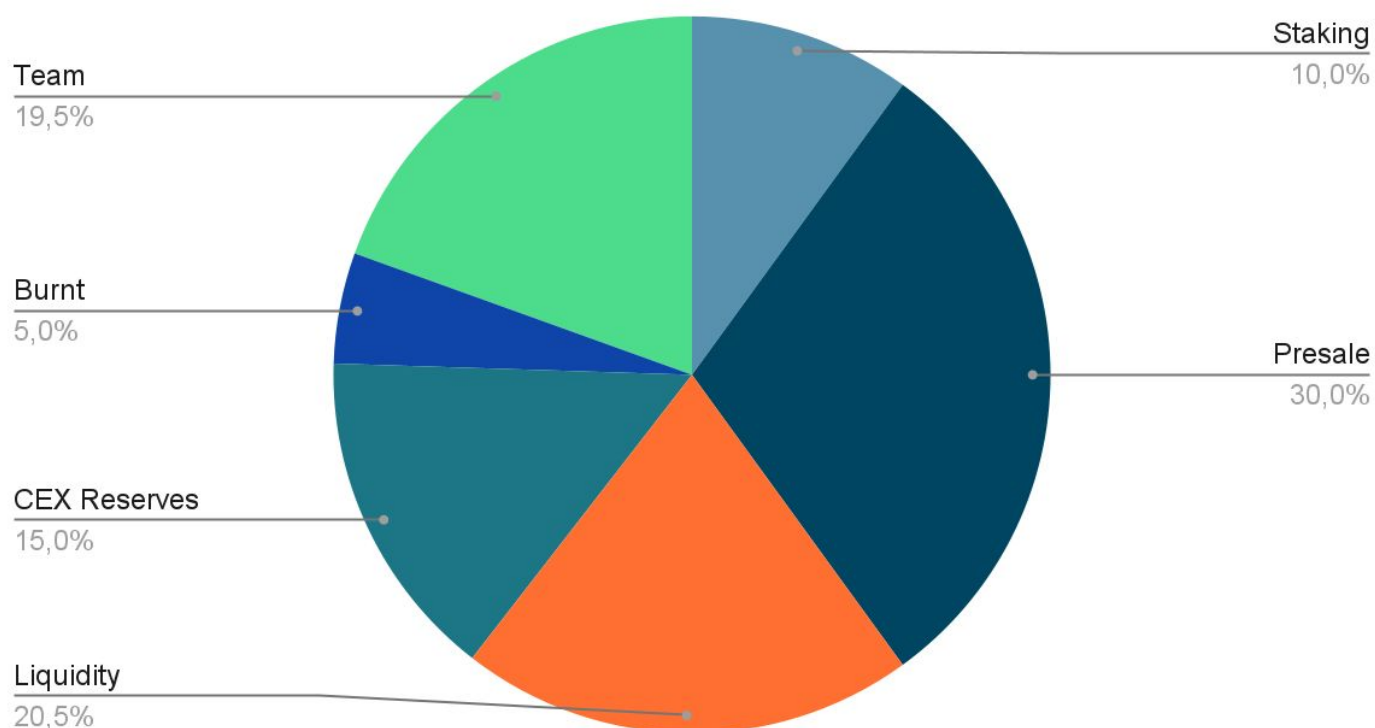
Team
19,5%

THE TEAM

The team has privately doxxed to PINKSALE

Rich Doge Poor Doge Fair Launch Audit KYC Upcoming

THE FIRST EVER⚡FART 2 EARN POOTYCALL⚡REAL WORLD INFLUENCER OWNER Charity Project aimed at restoring confidence in BSC. Fully doxxed owner and team. Most transparent project on BSC. ✅Huge partners ✅No team tokens ✅KYC & Audit

https://www.pinksale.finance/launchpad/0x58D9e10895Ec045Fb9e95E9566A2E00EAB24E993?chain=BSC

11

Website URL
https://rpdoge.com

Domain Registry
http://tucowsdomains.com

Domain Expiration
Expires on 2024-07-08

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page, appropriate color scheme, disturbing moving parts.

Content
There is not much information to help new investors understand what the product does right away. No grammar mistakes found .

Whitepaper
⚠️ No whitepaper.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?

Yes

RICH DOGE
POOR DOGE

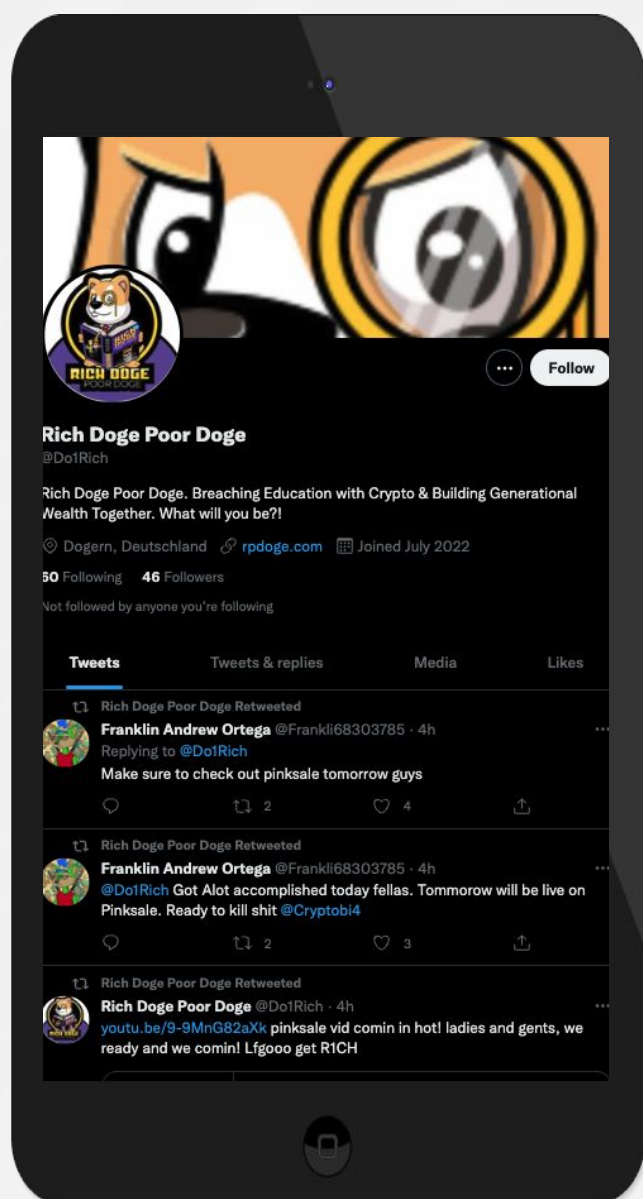BUY TOKEN   WOOF PAPER

rpdoge.com

SOCIAL MEDIA
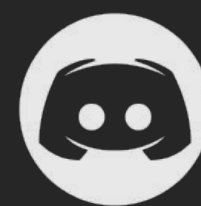## & ONLINE PRESENCE

ANALYSIS

Project's social media channels are active on daily basis.

Twitter

@Do1Rich

- 46 followers
- Very active
- Posts and retweets frequently

Discord

https://discord.com/invite/HhMPcxaSJK

- 13 members
- Few active members

Telegram

@rpDoge

- 400 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF
CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✔ **OVER 150 SUCCESSFUL CLIENTS**
- ✔ **MORE THAN 500 SCAMS EXPOSED**
- ✔ **MILLIONS SAVED IN POTENTIAL FRAUD**
- ✔ **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- ✔ **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to contact@spywolf.co or t.me/joe_SpyWolf

FIND US ONLINE

🌐 **SPYWOLF.CO**

🌐 **SPYWOLF.NETWORK**

✈ **@SPYWOLFNETWORK**

✈ **@SPYWOLFOFFICIAL**

🐦 **@SPYWOLFNETWORK**

⌗ **@SPYWOLFNETWORK**

14

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.